Attachment B: Owner/Operator CIP Checklist

Identify Critical Assets

- ❑ Physical assets
- ❑ Human assets
- ❑ Cyber assets
- ❑ Look across assets and sectors for critical interdependencies
- ❑ Criticality based on mission objectives of the system
- ❑ Criticality based on consequences

In determining consequence, review the following affects:

- ❑ The surrounding population – e.g., catastrophic health effects or mass casualties, or even loss in morale and public confidence in the government
- ❑ Public and governmental service – e.g., the inability of government agencies to perform essential missions, deliver essential public services, maintain public order, or ensure public health and safety
- ❑ The local and regional economy – e.g., due to disruption of the private sector's ability to deliver essential goods and services, or the negative impact on the economy through the cascading disruption of other critical infrastructure and key resources
- ❑ The environment – e.g., devastating impacts on local natural resources

Keep track of such assets and related information, such as:

- ❑ Basic asset data (e.g., asset name, location, owner, and function)
- ❑ System components that are central to the mission and function
- ❑ Dependencies (on what the asset depends in order to function)
- ❑ Results of vulnerability analyses
- ❑ Continuity, redundancy (including backups), and resiliency built into the asset
- ❑ Existing protective actions (e.g., fencing, biometrics, firewalls, procedures, etc.)

Assess Risk

- ❑ Conduct a threat analysis. Determine what type of risk the following threats pose to your assets:
  - ❑ Car or truck bombs
  - ❑ Firearms
  - ❑ Shoulder-fired missiles, rocket-powered grenades, etc.
  - ❑ Chemical weapons
  - ❑ Biological weapons
  - ❑ Nuclear weapons
  - ❑ Explosives

- Radiological weapons (e.g., nuclear "dirty bombs" – dispersal of radioactive material)
- Aircraft crashing into the asset or used as a platform to deliver other types of weapons (e.g., explosives, chemical, biological, or nuclear)
- Insider or expert knowledge to disable or destroy critical systems or to release hazardous materials (e.g., cyber attacks, release of hazardous materials from a chemical plant or refinery)
- Theft to acquire materials for use in future attacks
- Disruption of communications and control (e.g., SCADA, communications cables)
- Damage caused by improper operation or maintenance

- Determine risks posed by individual assets or groups of assets;
- Determine risks within a sector due to interdependencies among the assets in that sector

  Determine risks across sectors and across regions or the nation.
- Conduct vulnerability assessments.
- Determine probability of successful exploitation of the vulnerability.
- Combine the results of the Threat, Vulnerability, Consequence, and Probability Assessments into a single Risk analysis.

Prioritize Assets

- Compare data from the risk analysis within and across sectors
- Conduct benefit-cost analysis
- Adhere to an accepted prioritization process

Implement Protective Programs

- Develop a coordinated plan for protection, which has actions that fall into one or more of the following general categories for threat-based and threat-neutral situations:
  - Deter
  - Devalue
  - Detect
  - Defend
- Collaborate with organizations within and across sectors to develop Regional strategies to reduce vulnerability and prevent disruptions in service.
- Consider some of the following solutions:
  - Physical security, including extension of security perimeter beyond the limits of facility to create a buffer zone
  - Roving security inspections
  - Access control
  - Background checks for employees, temporary workers, contractors, subcontractors, security force, and potential first responders
  - Loss prevention, material control, and inventory management
  - Delivery service verification (e.g., request delivery worker identity card)

- ❑ Control-room security
- ❑ Policies and procedures
- ❑ Information/cyber security
- ❑ Intelligence, particularly for specific assets (e.g., East Coast vs. West Coast)
- ❑ Training on security plans
- ❑ Drills involving employees, contractors, public, and media
- ❑ Crisis management and emergency response, including incident command system
- ❑ Communication of hazards by asset owners to public sector protection forces

Request Assistance from Region 6

If your organization needs assistance in establishing the appropriate protective measures due to a lack of resources:

- ❑ Provide the CIP Work Group with information on the asset, its vulnerabilities, and recommendations for protection to include:

Asset Information

- ❑ Asset name and address or general description of location (e.g., meat processing facility ABC, XYZ Inc., etc.)
- ❑ Owner/operator name and address (e.g., ABC Company, contact person, address, telephone number, etc.)
- ❑ Sector (e.g., transportation, energy, etc.)
- ❑ Asset class or sub-sector (e.g., transportation-marine, etc.)
- ❑ Tracking/identification number (if applicable)
- ❑ Seasonality/frequency of use
- ❑ Function within the infrastructure (e.g., XYZ Inc. makes batteries for missiles).
- ❑ System components that are central to the mission and function (names of major systems)
- ❑ Dependencies (e.g., what does the asset depend on to function?)
- ❑ Continuity and redundancy to include back-ups built into the asset.
- ❑ Existing protective measures (e.g., fencing, biometrics, firewalls, etc.).

Vulnerability Information

- ❑ Specific vulnerability assessment related to the asset in question.
- ❑ Estimate of the asset's attractiveness or likelihood to be targeted by terrorists (typically closely related to the consequence), or an estimate of the asset's probability of being disrupted or destroyed by other means.

Consequence Information

- ❑ Results of a Consequence Analysis to include the effects of disruption or destruction on:

- Other infrastructure assets—interdependencies (e.g., what depends on it: people, physical assets, information technology, telecommunications, other sectors, etc.?).
- The regional economy.
- Public health and welfare.
- The public psyche.
- National or regional security.
- Estimate of the likelihood/probability that an attack on the asset would result in the predicted consequences.

Protective Measure Recommendations

- Specific protective actions for which the owner/operator seeks resources from the government.
- Specific protective measure for each vulnerability in question, to include acquisition data (cost, timing, etc.).
- Discussion of how each protective alternative will address the problem and the likelihood of the action's effectiveness in eliminating the vulnerability.
- Cost-benefit analysis for each protective alternative.

Assess Effectiveness

- Develop criteria to measure the effectiveness of protective actions.
- Develop measures around the specific objectives of each protective action.
- Affirm that specific goals are being met.

  Determine corrective actions as necessary.
- If you are a recipient of Region 6 funds or resources, submit a status report on the effectiveness of protective measures.

Share Information and Coordinate with Government and Private Sector Entities

- Collectively set standards for infrastructure security within each sector.
- Share best practice information with other owner/operators.
- Prepare for information sharing and collaboration by developing a common approach to risk management-based vulnerability reduction and asset protection.
- Participate in information exchanges within and among sectors, and with the Region 6 CIP Work Group by sharing protection gaps, resource needs, and (as appropriate) vulnerabilities and asset information.
- Share appropriate contact information within and across sectors to facilitate independent coordination and guarantee emergency communications.
- Work with the Region 6 CIP Work Group to develop incentive programs to encourage voluntary implementation of protective measures.
- Report any incidents or suspicious activity to local, State, or Federal law enforcement.

- ❑ Actively participate in existing sector-wide and national information sharing networks (e.g., trade associations, ISACs, Sector Coordinating Councils, NWWARN).

Become a CIP Leader in Your Sector

- ❑ Become an active member of your sector's information sharing network.
- ❑ Volunteer to serve as your sector's representative to the Critical Infrastructure Protection Work Group.
- ❑ Encourage CIP strategies and best practices within your sector.
- ❑ Participate in response exercises coordinated by government agencies.
- ❑ Encourage owner/operators to participate in the Region 6 CIP effort and in information sharing and coordination mechanisms.